ABSTRACT OF THE DISCLOSURE

[0057] A system and method by which novel, malicious execution traces may be detected by applying a combination of finite automation and heuristic analysis techniques. Such execution traces may be obtained by instrumenting system-level operating system calls, as well as by other techniques, such as, but not limited to, reading error log files, such as Windows NT event logs. With proper instrumentation, known good and known malicious programs may be run and their execution traces monitored. From such monitoring, a model may be derived, which can indicate those execution traces typically associated with malicious software. With this information, novel malicious programs which invoke execution traces similar to known malicious traces may be detected, and such programs may be stopped before significant damage can occur.

Document #: 1150288 v.1